Synthesizing Formal Models of Hardware from RTL for Efficient Verification of Memory Model Implementations

Flowchart: Automated translation from Verilog to μspec models

**A Taxonomy for Constructing Complete μspec Models**

- **μspec models** specify the space of all possible micro-architectural happens before graphs (μhb graphs) using first-order logic axioms that, given a program and a microarchitecture, instantiate
  - **μhb nodes**: Microarchitectural events, i.e., (instruction, location) pairs
  - **μhb edges**: Happens-before (HB) relationships between nodes

**Case Study Result**

- Performance comparison of rtl2μspec-assisted versus RTLCheck [1]-based verification of hardware MCMs (avg: 7.36 sec vs 25 min)

**Conclusion & Contribution**

- **Define what constitutes a complete μspec model for an RTL design**
- **rtl2μspec tool** for synthesizing complete, and proven correct by construction, μspec models from RTL with minimal user-intervention
- **Verification** of the RISC-V multi-V-Scale MCM implementation: rtl2μspec synthesizes a μspec model in 6.84 mins, during which a new bug is found. Subsequent Check-based verification takes less than 1 second per litsm test.

---

1. [https://check.cs.princeton.edu/](https://check.cs.princeton.edu/)